

REMARKS

The final Office Action mailed November 27, 2007 ("Final Action") rejects Claims 45-52 under 35 U.S.C. § 101 as allegedly claiming non-statutory subject matter. Final Action, p. 2. In particular, the Final Action states:

Claim 45 is computer programs claimed as computer listings "per se" that is, the descriptions or expression of programs are not physical "things". They are neither components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed components of a computer which permit the computer program's functionality to be realized. Therefore, claim 45 recites non-statutory subject matter.

Final Action, p. 3.

Respectfully, the Final Action misapplies the standard for evaluating such claims. In particular, as discussed in MPEP §2106.01:

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, **"functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component.** (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data.

Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. ***When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized.*** Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)(discussing patentable weight of data structure limitations in the context of a statutory claim to a data structure stored on a computer readable medium that increases computer efficiency) and *Warmerdam*, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with *Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure *per se* held nonstatutory). (Emphasis added)

Contrary to the assertions of the Final Action, Claim 45 does not claim "a computer program listing per se." Rather, Claim 45 claims functional descriptive material recorded on some computer-readable medium, specifically: "computer program code program code comprising

program code configured to sequentially poll a plurality of devices of the networked computer system for data relating to network communications thereof; program code configured to detect an anomaly responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and program code configured to determine a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device." Thus, Claim 45 meets the requirements of 35 U.S.C. §101 as outlined in MPEP §2106.01. Therefore, Applicant respectfully submits that the §101 rejections of Claims 45-52 are erroneous and should be withdrawn.

Claims 29, 31-35 and 43-52 are patentable

Independent Claims 29 and 45 stand rejected as being allegedly obvious over a combination of U.S. Patent Application Publication No. 2003/0110392 to Aucsmith et al. ("Aucsmith") and U.S. Patent No. 6,834,304 to Nisbet et al. ("Nisbet"). In particular, in rejecting Claim 29, the Final Action alleges that Aucsmith teaches all of the recitations of Claim 29 except "polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof." Final Action, p. 5. The Final Action asserts that Nisbet provides the missing teachings at Figs. 1 and 2 and at column 2, lines 23-30 and 39-42, stating "it would have been obvious . . . to combine Nisbet with Aucsmith, since one would have been motivated to identify malfunctioning network elements [Nisbet, col. 1 line 67, col. 2 line 1]." Final Action, p. 5.

Applicants respectfully traverse this rejection because there is no evidence from the prior art of a motivation to combine the malfunction detection described in Nisbet with the intrusion detection described in Nisbet, and because, even if combined, Aucsmith and Nisbet do not teach or suggest all of the recitations of Claim 29. Nisbet relates to a "system and method for auditing an optical network to identify malfunctioning network elements and to generate a report which would allow skilled personal to quickly and effectively identify areas of functionality of a deployed network element that is operating incorrectly by reading through the report." Thus, *Nisbet relates to detecting device malfunction, not intrusion*

detection. The passage from Nisbet cited as allegedly teaching "polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communications thereof" states:

In a first aspect, the present invention provides a method of auditing an optical communications network to determine operational states of network elements. The method consists of first retrieving operational data from a plurality of network elements. The data can be retrieved by polling the network elements via a serial connection, using, for example, a modem, or by accessing static data capture files. Next, the operational data is evaluated to determine an operational parameter for a given network element. In a presently preferred embodiment, the operational data is evaluated by processing network interface command lines within data capture files. If the operational parameter is determined to be invalid, it is flagged as an invalid operational parameter. To determine if the operational parameter is invalid, it can be compared to predetermined operational specifications for the given network element. If the operational parameter falls outside a predetermined operating range, it is considered invalid. The evaluation and determination steps are repeated for all operational parameters related to the given network element, and then again for each remaining network element. Once the evaluation is completed, a findings report is generated. The findings report lists any of the plurality of network elements determined to have at least one invalid operational parameter, displays details of each invalid operational parameter, and provides a finding status for each invalid operational parameter.

Nisbet, column 2, lines 21-47. The material from Nisbet cited as allegedly providing a motivation to combine states:

It is, therefore, desirable to provide a method of auditing a network to identify the operational parameters of network elements, particularly malfunctioning network elements, and to generate a report which allows skilled personnel to quickly and effectively identify areas of functionality of a deployed network element that is operating incorrectly by reading through the report.

Nisbet, column 1, line 66 through column 2, line 5. There is nothing here that relates to use of the "operational data" for any type of operation that involves detecting and predicting events, such as intrusions, that may span across multiple devices. Rather, Nisbet appears limited to detecting malfunctions of individual devices. Thus, the cited material provides no evidence of a motivation or suggestion to combine polling for data indicative of device malfunction as described in Nisbet with intrusion detection as described in Aucsmith.

Moreover, even if there were such a motivation or suggestion to combine, the combination of Aucsmith and Nisbet would not teach or suggest all of the recitations of Claim 29. Claim 29 recites:

A method of anticipating a device in a networked computer system is to be affected by an anomaly, comprising:

polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communications thereof;

detecting an anomaly responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and

determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device.

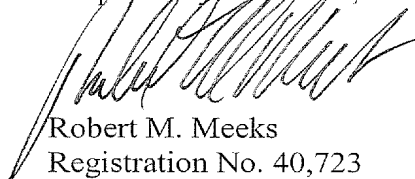
Aucsmith describes a variety of different actions that may be taken in response to detection of an anomaly (see Aucsmith, paragraphs [0048-0058] but, as conceded by the Final Action, Aucsmith does not teach any relationship of anomaly detection to polling. For example, none of the post-anomaly detection actions described in paragraphs [0048-0058] of Aucsmith appears to involve "determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device." Nisbet does not supply such teachings because, as noted above, Nisbet is limited to detecting failures of individual devices, and does not describe any type of operation that involves detecting and predicting events, such as intrusions, that may span across multiple devices.

Accordingly, even if combined, Aucsmith and Nisbet do not teach or suggest all of the recitations of independent Claim 29. For at least these reasons, Applicants submit that independent Claim 29 is patentable. Applicants further submit that independent Claim 45 is patentable for at least similar reasons. Applicants submit that dependent Claims 31-35, 43, 44 and 46-52 are patentable at least by virtue of the patentability of the respective ones of independent Claims 29 and 45 from which they depend.

Conclusion

Applicants submit that all of the claims are in condition for allowance for at least the reasons discussed above. Applicants respectfully request allowance of the claims and passing of the application to issue in due course. Applicants urge the Examiner to contact Applicants' undersigned representative at (919) 854-1400 to resolve any remaining formal issues.

Respectfully submitted,



Robert M. Meeks
Registration No. 40,723
Attorney for Applicants

USPTO Customer No. 39072
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on March 14, 2007.



Candi L. Riggs